

## **REMARKS**

Claims 1-3, 6-9, 11-12, 14-57, 59-69, and 71-74 are currently pending in the application. Claim 1 has been amended. Applicant submits that the amendment to claim 1 does not raise any new issues of patentability.

### **35 U.S.C. § 103 Rejections:**

Claims 1-3, 6-9, 11-12, 16-20, 26-27, 29-32, 46-57, 59-61, 69 and 71-74 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Edwards, U.S. Patent Application Publication 2004/0059825, in view of IEEE 802.11 ('IEEE'). Claims 14-15, 21-25, 28, 33-35, 39-45, 62 and 65-68 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Edwards in view of IEEE and in further view of non-patent literature by Cox. Applicant respectfully traverses these rejections.

**The cited references, taken singly or in combination, fail to teach or suggest all of the elements of the independent claims.** Independent claim 1 recites, in pertinent part:

A method of performing encrypted WLAN (Wireless Local Area Network) communication, the method comprising: operating driver software to perform a connection set-up for said encrypted WLAN communication; and operating a WLAN chip to perform data frame encapsulation and decapsulation during said encrypted WLAN communication ...wherein said data frame encapsulation and decapsulation is performed on a single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software, wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames intended for said data frame encapsulation from driver software... wherein performing said encrypted WLAN communication further comprises selecting one of the plurality of data frames for said data frame encapsulation by performing a

prioritization algorithm implemented on the **single-purpose hardware**.  
(Emphasis added).

Independent claims 46, 69, and 71 recite combinations of features that include elements similar to those highlighted above.

In the office action, the Examiner contends that Edwards teaches the element “wherein performing said encrypted WLAN communication further comprises selecting one of the plurality of data frames for said data frame encapsulation by performing a prioritization algorithm implemented on the single-purpose hardware,” citing paragraph [0052]. However, paragraphs [0052] and [0053] of Edwards contradict the Examiner’s assertion. Paragraphs [0052]-[0053] of Edwards state the following:

[0052] Hardware-based MAC component 24B may be configured to pull packets from queues 36, 38 on a selective basis. For example, software-based MAC component 24A may load configuration registers associated with hardware-based MAC component 24B to **assign priorities** to queues 36, 38. In this manner, hardware-based MAC component 24B, and particularly transmit logic 34, may be configured to expedite transmission of time critical packets such as beacons, which may be written to one of queues 36, 38 designated as high priority. In particular, transmit logic 34 may be configured to pull packets exclusively from one queue 36, 38 or the other, or to pull packets from both queues with a higher priority given to one of the queues. In addition, multiple queues 36, 38 can be used to separate packets that should be transmitted in an announcement traffic indication message (ATIM) period from those that should not. Also, hardware-based MAC component 24B may be capable of processing the packets according to quality of service (QoS) designations for the packets. [0053] **Software-based MAC component 24A formats and prioritizes packets that are to be sent out over the air interface before the packets are transmitted to hardware-based MAC component 24B.** In addition, software-based MAC component 24A may be configured to selectively write packets into one of queues 36, 38 based on priorities or time dependencies associated with the packets. Software-based MAC component 24A also may have a number of virtual queues to assist QoS functions prior to transmission of packets to the hardware-based MAC component. If software-based MAC component 24A runs on host processor 28, hardware-based MAC component 24A may require less processing and memory resources. If software-based MAC component

24A runs on an embedded processor 39, the MAC layer may benefit from added flexibility. (Emphasis added).

In paragraph [0053] as cited above, Edwards clearly states that software-based MAC component 24A prioritizes packets before these packets are transmitted to the hardware-based MAC component 24B. In paragraph [0052], Edwards states that software-based MAC component 24A may load configuration registers associated with hardware-based MAC component 24B to assign priorities to queues 36 and 38. However, nowhere in the above citation of paragraphs [0052] and [0053], or elsewhere in Edwards, is there any teaching or suggestion that hardware-based MAC component performs any prioritization of packets. Accordingly, Edwards fails to teach or suggest the element of “performing a prioritization algorithm implemented on the single-purpose hardware” as recited in claim 1 and similarly recited in the other independent claims. IEEE fails to provide any teaching or suggestion that taken singly or in combination with Edwards results in a combination of features that includes this element.

Edwards further fails to provide any teaching or suggestion of the element “wherein said data frame encapsulation and decapsulation is performed on a single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software.” In the office action, the Examiner contends encapsulation and decapsulation is associated with hardware-based MAC encryption and decryption. The Examiner appears to cite Fig. 4 of Edwards in support of this assertion. However, neither Fig. 4 nor its corresponding description in the specification provide any teaching or suggestion of “data frame encapsulation and decapsulation [] performed on a single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software.” With regard to Fig. 4, Edwards states the following:

[0046] FIG. 4 is a block diagram illustrating implementation of software-based MAC layer functionality in a host processor. As shown in FIG. 4, host 20 may include a central processing unit (CPU) 32, memory/bus controller 33 and host memory 35. CPU 32 runs communication applications that access WLAN station 18 to receive and transmit information via network 10. In addition, CPU 32 runs a driver 37 that drives WLAN station 18 via host interface 22 and memory/bus controller

33. Software-based MAC component 24A is implemented within driver 37, and provides a variety of MAC layer functionality using processing and memory resources resident in host 20. In this case, the implementation of a software-based MAC component 24A may reduce the processing and memory requirements on the board or chip carrying hardware-based MAC component 24B and other components of WLAN station 18.

Nothing in the above citation provides any teaching or suggestion of frame encapsulation or frame decapsulation, much less performing these functions on a hardware unit without executing instructions of driver software.

With regard hardware-based MAC component 24B, Edwards states the following in paragraph [0050]:

[0050] Host 20 may write packets directly into one or both of transmit queues 36,38 via the software-based MAC component 24A running within the driver software 37 executed by host CPU 32. In this manner, there is no need for additional memory for intermediate storage of packets within WLAN station 18. Instead, the only copies of the packets are stored in a respective transmit queue 36, 38. If there is a transmission failure, there is no buffered copy of the processed packet that experienced transmission failure. In other words, the hardware-based MAC component 24B does not store a copy of the processed packet, i.e., a packet subjected to encryption and other transmission processing. Instead, hardware-based MAC component 24B again pulls the unprocessed, raw packet that experienced transmission failure from the pertinent transmit queue 36, 38. Hardware-based MAC component 24B reprocesses the packet and attempts retransmission of the packet until transmission is successful or the maximum number of retransmission attempts specified by software-based MAC component 24A has been reached. Thus, a raw or unprocessed packet generally refers to a packet that has not been subjected to encryption, checksum generation or other transmission processing. In some modes of operation, software-based MAC component 24A may specify zero retransmission attempts by hardware-based MAC component 24B. In this case, instead of hardware-based MAC component 24B pulling a packet from one of transmit queues 36, 38, software-based MAC component 24A simply retransmits the raw, unprocessed packet across host interface 22 for reprocessing by hardware-based MAC component 24B. As will be described, the use of a command structure incorporating sequence numbers may be helpful in identifying pertinent packets for retransmission. (Emphasis added).

While the above citation makes reference to providing packets to hardware-based MAC component 24B, as well as the processing of packets by hardware-based MAC component 24B, no discussion of frame encapsulation or decapsulation is provided. In fact, Edwards provides no discussion whatsoever of frame encapsulation or frame decapsulation. Accordingly, Edwards fails to teach or suggest the element “wherein said data frame encapsulation and decapsulation is performed on a single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software” as recited in claim 1 and similarly recited in the other ones of the independent claims. Furthermore, IEEE fails to provide any teaching or suggestion that, taken singly or together with Edwards that would result in a combination of features that includes this element.

For at least the reasons given above, Edwards in view of IEEE fails to teach or suggest all of the elements of the independent claims, and thus a case of obviousness has not been established. Accordingly, removal of the 35 U.S.C. § 103(a) rejection is respectfully requested.

With respect to the remaining claims, Applicant notes that each of these claims depends from one of the independent claims discussed above. Thus, for at least the same reasons given above, Applicant submits that a case of obviousness has not been established, and thus respectfully requests removal of the 35 U.S.C. § 103(a) rejections.

**Official Notice:**

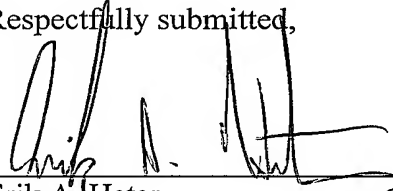
The Examiner takes Official Notice that IEEE 802.11b defines the LAN to have a radio frequency centered at 11 mHz. Applicant respectfully disagrees. IEEE 802.11b defines a transmission bit rate of 11 Mbit/second. Applicant also notes that IEEE 802.11 defines a spectral mask wherein a signal is attenuated by at least 30 dB from its peak energy at  $\pm 11$  MHz from the centre frequency. Applicant respectfully requests the Examiner produce authority in support of the Official Notice or withdraw the Official Notice.

**CONCLUSION**

Applicant submits the application is in condition for allowance, and an early notice to that effect is requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5800-00601/EAH.

Respectfully submitted,



Erik A. Heter  
Reg. No. 50,652  
AGENT FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.  
P.O. Box 398  
Austin, TX 78767-0398  
Phone: (512) 853-8800

Date: 2/25/06